

DEC 28 2006

Application No. 10/615,065
Amendment dated December 28, 2006
Reply to Office Action of September 28, 2006

Docket No.: 4444-0294PUS1

REMARKS

Claims 1-3 and 5-10 are now present in this application.

The specification and claims 1-3 and 5-10 have been amended and claims 4 and 11 have been cancelled without prejudice or disclaimer. Reconsideration of the application, as amended, is respectfully requested.

Claim for Priority

The Examiner alleges that a certified copy of the foreign priority document, Taiwan Application 091137721, has not yet been received by the U.S. Patent and Trademark Office. It is respectfully submitted, however, that the certified copy of the priority document was previously submitted on July 8, 2003, and is available in the image file wrapper of the U.S. Patent and Trademark Office's Patent Application Information Retrieval (PAIR) system. It is respectfully requested that the Examiner confirm receipt of the certified copy of the foreign priority document in his next action.

Objection to the Drawings

The drawings stand objected to under 37 CFR 1.83(a), as allegedly not showing the steps of claim 1. With reference to the foregoing amendments to the claims, it is respectfully submitted that the steps disclosed in the claims are supported by the originally filed drawings. In particular, the steps of claims 1, 5 and 8 are shown in steps 5-6 of FIG. 4 and blocks 130 and 150 of FIG. 5. The steps of claims 2, 6 and 9 are shown by steps 4-5 of FIG. 4 and blocks 120 and 130 of FIG. 5. It is therefore respectfully submitted that no new matter is present in the foregoing

Application No. 10/615,065
Amendment dated December 28, 2006
Reply to Office Action of September 28, 2006

Docket No.: 4444-0294PUS1

amendments. Reconsideration and withdrawal of any objection to the drawings is therefore respectfully requested.

Objection to the Specification

The specification stands objected to for certain informalities. In view of the foregoing amendments, it is respectfully submitted that these informalities have been addressed. Reconsideration and withdrawal of any objection to the specification are respectfully requested.

Objections to the Claims

The claims stand objected to for certain informalities. In view of the foregoing amendments, it is respectfully submitted that these informalities have been addressed. Reconsideration and withdrawal of any objection to the claims are respectfully requested.

Rejection under 35 USC 112

Claims 1-11 stand rejected under 35 USC 112, second paragraph. This rejection is respectfully traversed.

In view of the foregoing amendments, it is respectfully submitted that all claims particularly point out and distinctly claim the subject matter of the instant invention. Reconsideration and withdrawal of the 35 USC 112, second paragraph rejection are respectfully requested.

DEC 28 2006

Application No. 10/615,065
Amendment dated December 28, 2006
Reply to Office Action of September 28, 2006

Docket No.: 4444-0294PUS1

Rejection under 35 USC 101

Claims 1-11 stand rejected under 35 USC 101. This rejection is respectfully traversed.

The Examiner asserts that the claimed invention lacks patentable unity because no tangible result is obtained. Applicants respectfully disagree. The Examiner's attention is drawn to the "safe harbor" section of MPEP 2106(IV)(B)(2), which sets forth that:

"Another statutory process is one that requires the measurements of physical objects or activities to be transformed outside of the computer into computer data (In re Gelnovatch, 595 F.2d 32, 41 n.7, 201 USPQ 136, 145 n.7 (CCPA 1979) (data-gathering step did not measure physical phenomenon); Arrhythmia, 958 F.2d at 1056, 22 USPQ2d at 1036), where the data comprises signals corresponding to physical objects or activities external to the computer system, and where the process causes a physical transformation of the signals which are intangible representations of the physical objects or activities. Schrader, 22 F.3d at 294, 30 USPQ2d at 1459 citing with approval Arrhythmia, 958 F.2d at 1058-59, 22 USPQ2d at 1037-38; Abele, 684 F.2d at 909, 214 USPQ at 688; In re Taner, 681 F.2d 787, 790, 214 USPQ 678, 681 (CCPA 1982)."

Claims 1-3 of the present application are directed to a method for implementing the key modular exponentiation of a cryptographic operation in a computer system. The method outputs an encrypted digital message from a memory location of the computer system. Claims 5-7 and 8-10 are respectively directed to an apparatus and a computer-readable medium. The apparatus and a computer system capable of accessing the computer-readable medium are both for performing cryptographic operations on a digital message when they execute a program implemented by a programming language source embodying the method characterized by the features of claims 1-

Application No. 10/615,065
Amendment dated December 28, 2006
Reply to Office Action of September 28, 2006

Docket No.: 4444-0294PUS1

3. In view of techniques described in the specification, those skilled in the art will immediately appreciate that the disclosed invention can be preferably and advantageously implemented in a high-level programming language. It is respectfully submitted that the generation of the encrypted digital message is a practical application, and the method, apparatus, and medium of claims 1, 5 and 8 are structurally and functionally interrelated to the medium and therefore statutory, as they yield a useful, tangible, and concrete result. Reconsideration and withdrawal of the 35 USC 101 rejection are respectfully requested.

Rejections under 35 USC 103

Claims 1-11 stand rejected under 35 USC 103 as being unpatentable over Kocher et al., U.S. Patent 6,298,442, in view of Benoit, U.S. Publication 2003/0053621. This rejection is respectfully traversed.

Kocher provides a method to implement the modular exponentiation using essentially branchless routines such that the leakage of information is alleged to be minimized. The method set forth by Kocher performs the modular exponentiation in computer assembly language (or machine language) level, which can be appreciated by the low-level computer instructions such as XOR, AND, OR and ROR illustrated when embodiments are described (referring to mnemonics shown in FIG.1 and specification, especially, col.6, lines 24-32). Additional features of Kocher includes fixed memory pattern accessing to make memory bus access independent of the exponent key content and avoiding multiplication-by-1 operation to prevent external detection.

Application No. 10/615,065
Amendment dated December 28, 2006
Reply to Office Action of September 28, 2006

Docket No.: 4444-0294PUS1

Benoit provides an algorithm (or high-level programming language) level method for the modular exponentiation. Benoit contemplates keeping identical execution time of each iteration by using a flag which may be inverted in each iteration according to the value of a current examined exponent key bit.

It is respectfully submitted that Kocher and Benoit, either alone or in combination, fails to teach using the same variable for the modular-multiplying result and the multiplying multiplicand (referred to as the M-feature hereinafter, for simplicity) in two modular-multiplying operations. This feature makes the claimed method resistant to an M safe error attack if the two performing steps are the only modular-multiplying operations in an embodiment (i.e. if you embody the method in the disclosed algorithm of FIG. 4 and FIG. 5 without any major variation). It is noted that the modular-multiplying operation ($R=RQ \bmod n$) shown in Kocher (block 125, FIG.1) provides an M-feature. The present application, however, recites at least two modular-multiplying operations which meet with the M-feature. Moreover, Kocher will achieve the same effect even if the $R=RQ \bmod n$ in block 125 is rewritten as $R=QR \bmod n$. In other words, the M-feature found in the present application is neither taught nor suggested by Kocher, either explicitly or implicitly. In particular, using two modular-multiplying operations with the M-feature to implement the modular exponentiation is neither taught nor suggested by Kocher.

It is also respectfully submitted that the claimed performing steps are both executed "unconditionally" to achieve a branchless computer program. In other words, the claimed performing steps are always executed in each iteration of the loop for computing the modular exponentiation. It is a key feature of the present invention to work out a branchless algorithm

RECEIVED
CENTRAL FAX CENTER

DEC 28 2006

Docket No.: 4444-0294PUS1

Application No. 10/615,065
Amendment dated December 28, 2006
Reply to Office Action of September 28, 2006

which has all modular-multiplying operations complying with the M-feature to overcome various types of attacks.

With respect to claim 2, this claim recites altering the multipliers of the two multiplying operations of claim 1 based on the values of two adjacent bits of the secret exponent key. This limitation establishes the main loop of the modular exponentiation.

Turning to claim 3, this claim 3 recites that all the modular-multiplying operations therein comply with the M-feature.

The secondary reference to Benoit fails to overcome the above-noted deficiencies of the primary reference to Kocher.

For independent claims 5 and 8, it is noted that these claims should be allowable over the prior art of record for similar reasons to those set forth above in connection with independent claim 1.

In view of the foregoing amendments and remarks, it is respectfully submitted that the method, apparatus, and medium of claims 1, 5 and 8, as well as their dependent claims, are neither taught nor suggested by the prior art utilized by the Examiner. Reconsideration and withdrawal of the 35 USC 103 rejection are respectfully requested.

Conclusion

Favorable reconsideration and an early Notice of Allowance are earnestly solicited.

Because the additional prior art cited by the Examiner has been included merely to show the state of the prior art and has not been utilized to reject the claims, no further comments concerning these documents are considered necessary at this time.

Application No. 10/615,065
Amendment dated December 28, 2006
Reply to Office Action of September 28, 2006

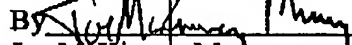
Docket No.: 4444-0294PUS1

In the event that any outstanding matters remain in this application, the Examiner is invited to contact the undersigned at (703) 205-8000 in the Washington, D.C. area.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Dated: December 28, 2006

Respectfully submitted,

By 
Joe McKinney Muncy
Registration No.: 32,334
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant